Timo Mattila

Palvelinympäristön rakentaminen ja yhdistäminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

28.4.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Timo Mattila Palvelinympäristön rakentaminen ja yhdistäminen 35 sivua 28.4.2015
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	yliopettaja Matti Puska

Insinöörityön aiheena on Comspot Oy:n asiakkaalle suorittama projekti kaksivaiheisesta palvelinympäristön rakentamisesta, uusien palveluiden käyttöönottamisesta sekä kahden eri tietojärjestelmän yhdistämisestä, jossa asiakkaan oma fyysinen palvelin sekä asiakkaan vuokraamat virtuaalipalvelimet TelecityGroup Oy:ltä siirretään ja niiden toimintaympäristö yhdistetään Comspot Oy:n palvelinkeskuksesta tarjoamiin virtuaalipalvelimiin.

Asiakkaan tietojärjestelmät ovat ennen projektin tekoa eriytetty kahdeksi eri järjestelmäksi, joiden molempien pohjana on käytetty Active Directory -hakemistopalvelinta, jotka molemmat tuottavat päällekkäisiä palveluita. Uuden palvelininfrastruktuurin rakentamisella ja sen yhdistämisellä uudistetaan, tehostetaan ja selkeytetään tietojärjestelmien hallinnointia ja toimintoja sekä vähennetään asiakkaalle kohdistuvia taloudellisia kustannuksia.

Työssä käsitellään projektin etenemistä suunnitteluvaiheesta toteutukseen. Asiakkaalle on tarkoitus luoda tietojärjestelmä, joka tukee Microsoft Office 365 - palveluiden käyttöä, luoden luottamussuhteen Active Directory -palvelimen ja Office 365 pilvipalvelun välille käyttäen kertakirjautumismenetelmää. Kertakirjautuminen mahdollistaa käyttäjän pääsyn useisiin eri palveluihin yhdellä käyttäjän todennuskerralla. Luottamussuhteen rakentamiseen käytetään Microsoftin kehittämää Active Directory Federation Services 2.0 -palvelua.

Ensimmäisessä vaiheessa rakennetaan asiakkaalle palvelininfrastruktuurin runko, johon projektin toisen vaiheen tietojärjestelmä yhdistetään. Työssä esitellään siihen käytetyt palvelimet, käyttöönotettavat palvelut ja työkalut, joilla projekti toteutetaan.

Palvelinten ja palveluiden asennus todetaan toimivaksi kun käyttäjä onnistuu kirjautumaan palveluihin ja jaettuihin resursseihin.

Projektin tuloksena asiakkaalla on käytössä uudistettu ja yhdistetty palvelinympäristö uusilla palveluilla.

Avainsanat	Palvelin, Verkkoinfrastruktuuri, Office 365, ADFS, Intune

Author Title Number of Pages Date	Timo Mattila Server infrastructure installation and merger 35 pages 28 April 2015
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructor	Matti Puska, Principal Lecturer

The goal of this bachelor's thesis is to describe a project carried out by Comspot Oy for its customer. The purpose of the project was to build a new network infrastructure, deploy new services and connect two different network topologies. In addition, the customer's own physical server and the customer's rented virtual servers from Telecitygroup Oy were to be merged with the datacenter of Comspot Oy.

Before the project started, the customer had two different information systems which both used the AD infrastructure producing the same kind of services. The new server infrastructure and merging two servers, gives the advantage of simplifying information system administration, increasing the performance and enhancing security with lower management costs.

This thesis covers the progress of the project from the planning to the installation. The first step of the project was to install a new server infrastructure which supports the Microsoft Office 365 cloud service and to create the Active Directory Federation Service between the Active Directory server and Office 365 service with the single-sign-on method. The Single-sign-on gives users access to multiple different services with a single authentication process. To create a federation between the Active Directory server and the Office 365 service, the Active Directory Federation Services 2.0, developed by Microsoft, was used.

In the first phase of the project, the basis of the server infrastructure was installed for the customer, whereas in the project's second phase the data information system was merged with the newly installed server infrastructure. Overall, this study demonstrates which servers, deployment of services and tools were used to accomplish the project.

The server and service installation are successful if the user is able to login to server infrastructure services and to its shared resources.

As a result, the customer has an updated network infrastructure with new services plus a merged server infrastructure.

Keywords	Server, Network Infrastructure, Office 365, ADFS, Intune

Sisällys

Lyhenteet

AD	Microsoft Active Directory. Windows Server -käyttöjärjestelmän toimialueen käyttäjjen ja työasemien tunnistautumis- ja hallintapalvelu
ADFS	Microsoft Active Directory Federation Services. Windows Server -käyttöjärjestelmän palvelu käyttäjän tunnistautumiselle Office 365 -palveluun
AIK	Windows Automated Installation Kit for Windows 7. Auttaa Microsoft Windows 7 ja Windows Server 2008 R2 -käyttöjärjestelmätuoteperheiden asennuksessa, mukauttamisessa ja käyttöönotossa
DA	Microsoft Direct Access. Windows Server -käyttöjärjestelmän rooli, joka luo suojatun yhteyden yrityksen verkkoon ilman erillistä VPN -asiakasohjelma kautta luotua yhteyden muodostamista.
DMZ	Demilitarized Zone. Fyysinen tai looginen aliverkko, joka on sijoitettu ulko- ja sisäverkon väliin tietoturvan lisäämiseksi.
DNS	Domain Name System. Nimipalveluilla muunnetaan verkkotunnukset IP-osoitteiksi.
CSV	Comma Separeted Values. Taulukkorakenteinen tekstitiedostomuoto, jonka taulukkorakenteen kentät on erotettu pilkuilla ja rivinvaihdoilla.
FQDN	Fully Qualified Domain Name. Täydellinen toimialuenimi työasemalle tai palvelimelle, joka sisältää vähintään ensimmäisen ja toisen tason verkkotunnuksen.
GPO	Group Policy Object. Toimialueen ryhmäkäytännöt, joilla määritetään sääntöjä käyttäjille ja työasemille.
HTTPS	Hypertext Transfer Protocol Secure. Suojattu siirtoprotokolla www-palvelinten ja selainten väliselle tietoliikenteelle.

IP	Internet Protocol. Verkkokerroksen protokolla IP-pakettien perille toimittamiselle pakettikytkentäisessä verkossa.
MPLS	Multiprotocol Label Switching. IP-pakettien siirtomenetelmä ennalta määritettyjen yhteyksien ylitse.
OU	Organizational Unit. Avustaa organisaation hierarkkisen kokonaisuuden rakentamisen Active Directoryn objekteista.
SSO	Single sign-on. Menetelmä, jossa yhdellä käyttäjän autentikointikerralla annetaan pääsy useisiin palveluihin.
SSL	Secure Sockets Layer. Salausprotokolla, jolla suojataan internetsovellusten tietoliikenne.
SQL	Structured Query Language. Relaatiotietokannan käyttämä kyselykieli.
URL	Uniform Resource Locator. Käytetään osoittamaan WWW-sivujen tiedon sijaintia
VCPU	Virtual Central Processing Unit. Palvelinkeskuksen fyysisestä suorittimesta määritetty näennäisprosessori virtuaalikoneelle.
VPN	Virtual Private Network. Erillinen virtuaaliverkko, jolla on mahdollista muodostaa suojattu yhteys julkisesta verkosta yritysverkkoon.

1 Johdanto

Projektissa on tavoitteena rakentaa asiakkaalle uusi palvelinympäristö, käyttöönottaa uudet palvelut ja yhdistää kaksi eri palvelinympäristöä yhdeksi kokonaisuudeksi. Palvelinympäristö on tarkoitus rakentaa Comspot Oy:n palvelinkeskukseen.

Palvelinympäristön yhdistämisen ensimmäinen osa koostuu asiakkaan omistaman ja omissa tiloissa sijaitsevan fyysisen palvelimen tietojen ja sen palveluiden siirtämisen Comspot Oy:n palvelinkeskuksesta vuokrattaville virtuaalipalvelimille. Asiakkaan paikallisen palvelimen Microsoft Exchange -sähköpostipalvelu siirretään Microsoft Office 365:een käyttäen ADFS (Active Directory Federation Services)- ja SSO (Single sign-on) -palveluja. Asiakkaalle asennetaan uuden palvelinympäristön vaativat virtuaalipalvelimet Comspot Oy:n tarjoamasta palvelinkeskuksesta ja niille asennetaan ADFS:n edellyttämät palvelut. Asiakkaan toimitiloihin asennetaan Site-to-site VPN (Virtual Private Network) -yhteys, jolla työasemat pääsevät käyttämään toimitiloistaan palvelimien resursseja. Lisäksi käyttöönotetaan Direct Access 2012 -palvelu, joka mahdollistaa etäkäyttäjien pääsyn palvelinten resursseihin. Projektin yhteydessä asiakkaan käyttämien työasemien käyttöjärjestelmät päivitetään Windows 7 Enterprise -versioiksi ja käyttäjäprofiileihin tallennetut tiedot siirretään uudelle AD (Active Directory) -käyttäjälle. Office 365 käyttöönotossa käytetään Microsoft Office 365 Deployment Guide -ohjeistusta, jonka Microsoft oli toimittanut projektia varten. Asiakkaalla on kaksi alaorganisaatiota, joiden yhdistämiselle odotetaan hyväksyntää ja joiden tietojärjestelmät ovat eriytetty tarkoituksellisesti. Alaorganisaatioilla on käytössä kaksi erillistä AD-toimialuetta sekä verkkoinfrastruktuuria, jotka on tarkoitus yhdistää samaksi AD-toimialueeksi.

Ensimmäisen työvaiheen päätyttyä asiakkaan omistama palvelin poistetaan käytöstä ja ensimmäisen alaorganisaation työasemat liitetään uuteen toimialueeseen. Samalla otetaan tuotantokäyttöön uusi palvelininfrastruktuuri uusilla palveluilla. Ensimmäisen työvaiheen aikana rakennetaan pääsääntöinen palvelinympäristö, johon projektin toisen vaiheen palvelinympäristö yhdistetään. Ensimmäisen työvaiheen verkkolaitteet, työasemat, palvelininfrastruktuuri ja palvelut dokumentoidaan ja luovutetaan asiakkaalle. Projektin toinen vaihe jää odottamaan asiakkaan päätöstä ja ilmoitusta ajankohdasta palvelinympäristön yhdistämisestä.

Projektin toinen vaihe sisältää asiakkaan toisen alaorganisaation vuokraamien virtuaalipalvelinten ja niiden tietojen siirtämisen Comspot Oy:n palvelinkeskukseen, joka yhdistetään projektin ensimmäisen vaiheen aikana rakennettuun palvelinympäristöön. Lisäksi siirretään Nebula Oy:n kautta hankitut sähköpostipalvelut käytössä olevaan Office 365 -palveluun.

Toisen työvaiheen päätyttyä asiakkaalla on käytössään yhdistetty palvelinympäristö ja sen tuottamat palvelut. Telecitygroup Oy toimii asiakkaan palvelinverkon palveluntarjoajana. Sen tarjoaman MPLS (Multiprotocol Label Switching) -verkko on yhdistetty Comspotin palvelinkeskukseen, johon liitetään projektin ensimmäisessä vaiheessa luotu palvelinverkko. Telecitygroup Oy:n virtuaalipalvelimet poistetaan käytöstä, ja Nebula Oy:n tarjoama sähköposti-palvelu lopetetaan. Toisen työvaiheen verkkolaitteet, työasemat, palvelininfrastruktuuri ja palvelut dokumentoidaan ja luovutetaan asiakkaalle.

2 Comspot Oy:n palvelinkeskus ja palveluiden tarjonta

Comspot Oy:n palvelinkeskus tarjoaa asiakkaille resursseja yksityisestä korkean saatavuuden palvelinpilvestä. Palvelinkeskus on suunniteltu skaalautuvaksi myös suuriin tarpeisiin.

Comspot Oy:n palvelinkeskus rakentuu IBM BladeCenter -palvelinlaitteistosta ja Hitatchi Universal Storage Platform -levynhallintajärjestelmästä sekä muista verkkoliikenteen laitteista. Palvelinten virtualisointi on toteutettu Citrix Xen Server -virtualisointialustalla. Laitteisto sijaitsee Telecitygroup Oy:ltä vuokratuissa palvelinsalitiloissa. Yritys huolehtii monitasoisesta fyysisestä turvallisuudesta ja pääsynhallinnan valvonnasta.

Palvelinkeskuksen verkko on rakennettu vikasietoiseksi käyttäen useita rinnakkaisia laitteita. Verkkoyhteydet palvelinkeskuksen ja ulkomaailman välillä voidaan toteuttaa usean eri operaattorin kanssa, jolloin yksittäisellä operaattorilla oleva sisäinen vika ei aiheuta haittaa asiakkaidemme palveluille. Palvelinkeskuksen asiakkaan verkkoinfrastruktuuri on erotettu muista oman virtuaaliverkon avulla.

Comspot Oy on IT-talo, joka tarjoaa seuraavanlaisia palveluita [1]:

- Hosting-palvelut
- ulkoistettu tietohallintopalvelu
- IT-tuki ja ylläpitopalvelut
- konsultointi
- verkkosivujen suunnittelu ja toteutus
- Microsoft Office 365:n käyttöönotto ja tuki
- virtuaalipalvelimet
- etävarmuuskopiointi
- Lemonsoft-toiminnanohjausjärjestelmän käyttöönotto ja tuki
- laitteistomyynti
- palomuuripalvelut.

3 Office 365

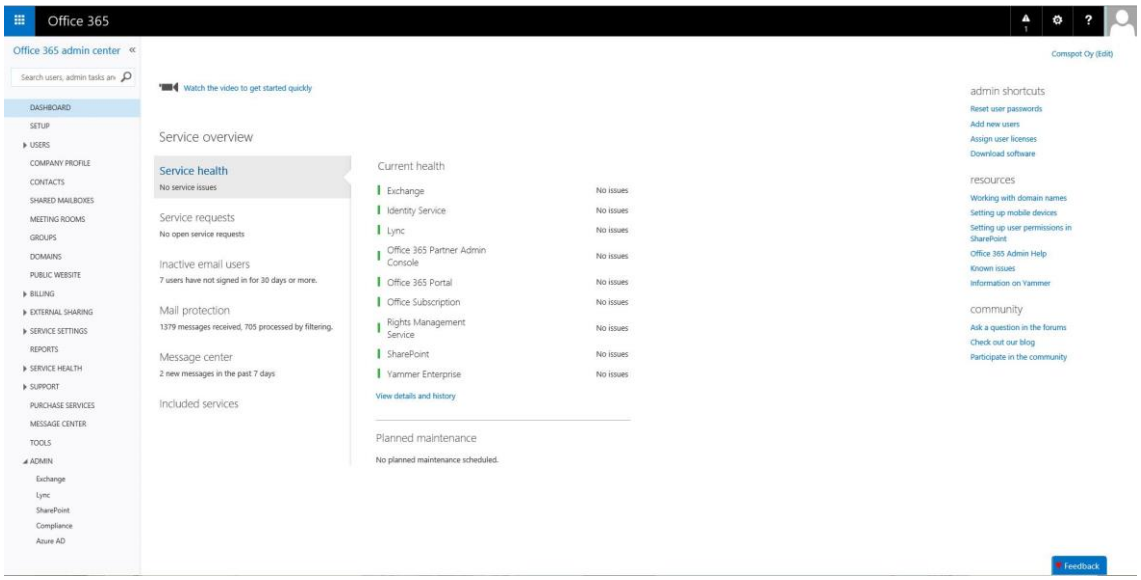
Microsoft Office 365 on Microsoftin ylläpitämä SaaS (Software as a service) tyyppinen pilvipalvelu, josta tilaaja saa hankittua Microsoftin sähköiset toimistosovellukset ja viestintäpalvelut. Office 365 julkaistiin edeltäjänsä BPOS (Business Productivity Online Suite) -ohjelmiston seuraajaksi vuonna 2011 kilpailemaan Google Apps -palvelun kanssa.

Office 365 on modulaarisesti rakennettu kokonaisuus, joka tarjoaa tilaajalle uusimman saatavilla olevan version sisältämistään ohjelmistoista. Office 365 kautta saatavat palvelut tarjoavat tyypilliset SaaS -palveluiden edut, joita esimerkiksi ovat ohjelmistojen edulliset aloituskustannukset, ohjelmistojen käyttö melkein millä tahansa laitteella, jossa on Internet-yhteys ja verkko-selain, ohjelmiston infrastruktuurin tarpeettomuus tilaajalle ja palvelun tarjoajan ylläpito ja tuki palveluihin. Office 365 kautta tilattavat palvelut

laskutetaan käyttäjäkohtaisesti joko kuukausittain tai vuosittain. Kuvassa 1 on esitetty Office 365 -palvelun hallintapaneeli, joka on käytössä palveluun määritetyille järjestelmänvalvojille.

Office 365 -palvelun kautta saatavat ohjelmistot [2]:

- Exchange
- Sharepoint Online
- Lync
- Project
- Visio
- Yammer
- Power BI
- Dynamics CRM.



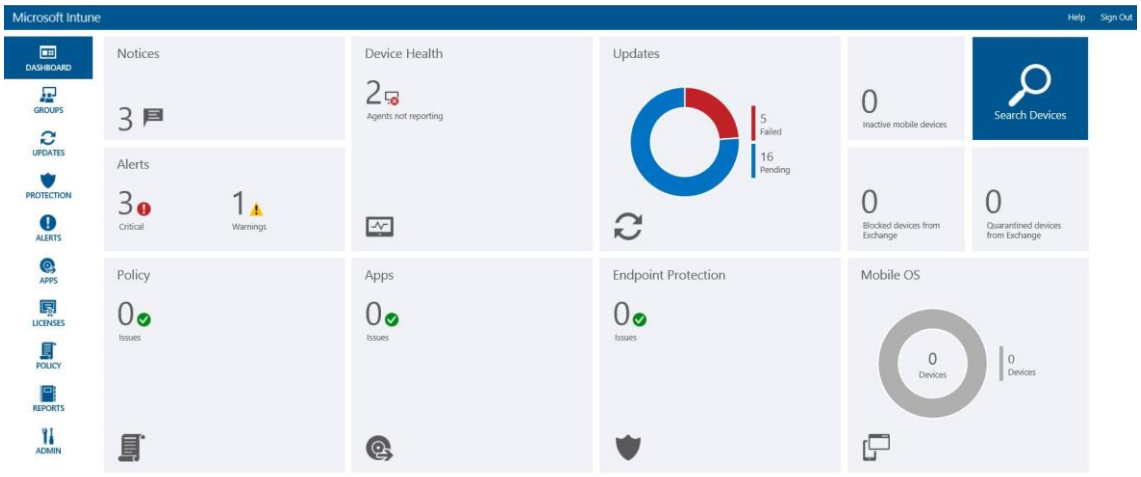
Kuva 1. Office 365 järjestelmänvalvojan hallintapaneeli.

4 Windows Intune

Windows Intune on Microsoftin vuonna 2011 julkaisema pilvipalvelu työasemien ja mobiililaitteiden hallintatyökaluksi. Windows Intune vaatii toimiakseen Internet-yhteyden ja asiakasohjelman asennuksen työasemalle. Mobiililaitteille on saatavissa Company Portal -sovellus, joka on asennettavissa tällä hetkellä Android-, iOS- ja Windows Phone 8.x -laitteisiin. Windows Intune -lisenssit laskutetaan käyttäjäkohtaisesti kuukausittain tai vuosittain. Kuvassa 2 on esitetty Windows Intune Admin Console -hallintapaneeli, joka on käytössä palveluun määritetyille järjestelmänvalvojille.

Windows Intune tarjoaa seuraavanlaisia ominaisuuksia [3]:

- laitteistoinventaario
- ohjelmistoinventaario
- Windows Update -päivitysten jakelu
- Microsoft Windows Endpoint Protection -virustorjuntaohjelmisto
- työasemien etähallinta
- ohjelmistojakelu *.EXE-, *.MSI-, *.APK-, *.IPA-, *.XAP-, *.APXX-, *.APPXBUNDLE -tyyppisille tiedostoille
- Company Portal -sivusto, josta selaimen kautta on ladattavissa sivustolle jakoon laitettuja ohjelmistoja
- työasemien käytäntöjen hallinta
- Remote tasks -tehtävien suorittaminen
- päivitysoikeudet Windows -käyttöjärjestelmiin (palvelupakettikohtainen ominaisuus).



Kuva 2. Windows Intune Admin Console Dashboard.

5 Ensimmäisen vaiheen projektisuunnitelma

Projektisuunnitelma pyrittiin tekemään vastaamaan asiakkaan tarpeita selkeästi ja johdonmukaisesti vaiheistettuna. Työvaiheet jaettiin kahdeksan työntekijän kesken siten, että ne vastaisivat jokaisen projektiin osallistujan omaan osaamispiiriin kuuluvaa aluetta. Toimin projektissa projektipäällikkönä ja vastuullani oli projektin suunnittelu, työvaiheiden ja työmäärien aikojen arviointi, resurssien jako ja projektin saattaminen alusta loppuun sekä toimiminen projektin työvaiheiden resurssina.

5.1 Palvelinympäristön ja palveluiden työvaiheet

Projektin työvaiheiden suunnittelun ja toteutukseen käytimme Microsoft Office 365 Deployment Guide for Enterprises -ohjetta [4], joka tarjoaa rakenteellista lähestymistapaa ja ohjeistusta työvaiheiden suorittamiselle. Projektin työvaiheet on listattu taulukkoon 1.

Taulukko 1. Projektin ensimmäisen vaiheen työtehtävät.

Task Name	WBS	Predecessors
Windows Intune käyttöönotto	**1**	
Intune-tilin luonti	1.1	
Lisätään Comspot-palvelun järjestelmän valvojaksi	1.2	
Suunnitellaan ja lisätään käyttäjät ja laiteryhmät	1.3	
Windows 7 Enterprise imagen teko	1.4	
Määritetään työasemien päivitysasetukset	1.5	
Windows 7 Enterprisen käyttöönotto työasemissa	**2**	
Käyttäjäprofiilien kopionti Easy Transferilla	2.1	
Windows 7 imagen asennus työasemiin	2.2	
Lisätään työasemat toimialueeseen	2.3	**4**
Microsoft Office 365:n käyttöönotto	**3**	
Office 365 -tilin luonti	3.1	
Lisätään Comspot-palvelun järjestelmän valvojaksi	3.2	
Migraation strategian valmistelu	3.3	
Käyttäjien tunnistus ja tilit	3.4	
Sähköpostilaatikon koon tarkistus	3.5	
Tarkistetaan käytettävät mobiilialustat	3.6	
Office 365:een toimialueen luonti ja vahvistus	3.7	
Office 365 -sähköpostimigraatio	**3.8**	
IMAP migration -tyyppinen migraation teko	3.8.1	**4**
Käyttäjien lisenssien määrittäminen	3.8.2	
Käyttöoikeuksien määrittäminen	3.8.3	4.3.5
SSO-aktivointi	3.9	**4**
Nimipalvelumuutokset	3.10	4.3.5
Infrastruktuurin palvelimet	**4**	
Esivalmistelut	**4.1**	
Paikallisen Active Directoryn valmistelu ja muokkausten tarpeet	4.1.1	
Suunnitellaan käyttäjät ja laiteryhmät	4.1.2	
AD-asennus	**4.2**	
AD-palvelinalustan asennus ja verkkomääritykset	4.2.1	
AD DS -roolin asennus	4.2.2	
Lisätään käyttäjät -ja laiteryhmät ja siirretään toimialueen käyttäjät ja työasemat niihin	4.2.3	
GPO-määritykset	4.2.4	
ADFS-asennus ja konfigurointi	**4.3**	
ADFS-palvelinalustan asennus ja verkkomääritykset	4.3.1	
AD DS -roolin asennus	4.3.2	
ADFS 2.0:n asennus ja konfigurointi	4.3.3	
Sertifikaatin hankinta ja asennus	4.3.4	
Toimialueen kirjautumisen peruskustomointi	4.3.6	**4**
Tulostuspalvelun roolin asennus	4.3.7	
ADFS Proxyn asennus ja konfigurointi	**4.4**	
ADFS Proxy -palvelinalustan asennus ja verkkomääritykset	4.4.1	
ADFS Proxy 2.0:n asennus ja konfigurointi	4.4.2	4.3.3
SSL-sertifikaatin asennus	4.4.3	4.3.4
Directory Synchronization -työkalun asennus ja synkronointi	4.4.4	
VPN-tunnelointi	**5**	**4**
Palomuurien konfigurointi	5.1	
Site-to-site VPN-määritykset Comspot palvelinkeskukseen	5.2	
MPLS verkon porttiavaukset Site-to-site VPN:lle	5.3	
Palomuurien asennus toimipisteisiin ja yhteyden testaus	5.4	
Henkilöstön koulutus ja ohjeistus Windows Office 365:n, Intunen, Lyncin ja Sharepoint Onlinen käyttöönotossa	**6**	
Office 365 ja Intune-ohjeiden dokumentointi	6.1	
Ensimmäinen henkilöstön Microsoft Office 365-,Intune-, Lync- ja Sharepoint -koulutus	6.2	
Toinen henkilöstön Microsoft Office 365-,Intune-, Lync- ja Sharepoint -koulutus	6.3	

Tietojärjestelmän dokumentointi	**7**	
Verkkoinfran ja laitteiston dokumentointi	7.1	
Online-palveluiden dokumentointi	7.2	
Käyttäjien dokumentointi	7.3	
Paikallisten ohjelmistojen dokumentointi	7.4	
Microsoft Direct Access 2012 asennus	**8**	**4**
DA-palvelinalustan asennus	8.1	
Direct Access and VPN (RAS) -roolin asennus	8.2	
DA-konfigurointi	8.3	
DA-käyttäjäryhmien määrittäminen	8.4	
SQL-tietokantapalvelimen asennus	**9**	**4**

Projektin toteutus sovittiin asiakkaalle sopivimmaksi ajankohdaksi. Alustavat työt sekä tehtävät, jotka eivät häiritse asiakkaan työskentelyä nykyisessä palvelinympäristössä, suoritettiin niin pitkälle kuin se oli mahdollista. Näihin kuuluivat palvelinten asennukset, palveluiden asennukset ja määritykset sekä uuden verkkoympäristön luonti. Uusi ympäristö otetaan tuotantokäyttöön työasemien uuteen toimialueeseen liittämisen jälkeen.

5.2 Office 365 -palvelusta käyttöönotettavat palvelupaketit

Office 365 -palvelusta valittiin asiakkaan tarpeita vastaavat palvelupaketit. Käyttäjille määritettiin Office 365 E1, E3 ja Exchange Online Kiosk -palvelupaketit, jotka tarjoavat taulukon 2 sisältävät ominaisuudet.

Taulukko 2. Office 365 -palvelusta käyttöönotetut palvelupaketit [5].

Office 365 -palvelupaketti	E3	E1	Exchange Online Kiosk
Office-sovellusten täydet versiot asennettu Word, Excel, PowerPoint, Outlook, Publisher ja OneNote viiteen PC- tai Mac-tietokoneeseen			
Office tableteissa ja puhelimissa käytä täyttä asennettua Officea enintään viidessä tabletissa ja viidessä puhelimessa			

Officen online-versiot mukaan lukien Word, Excel ja PowerPoint	●	●	
Tiedostojen tallentaminen ja jakaminen - 1 Tt tallennustilaa/käyttäjä	●	●	
Yritysluokan sähköposti, kalenteri, yhteystiedot ja 50 gigatavun Saapuneet-kansio *Exchange Online Kiosk 2 Gt Saapuneet-kansio	●	●	* ●
Rajoittamaton määrä verkkokokouksia, pikaviestejä ja HD-video-neuvotteluja. Sisältää Lync-sovelluksen	●	●	
Ryhmien käyttöön tarkoitettu intranetsivusto ja mukautettavat suojausasetukset	●	●	
Yrityksen yhteisöpalvelu (Yammer) auttaa eri osastoilla ja eri toimipisteissä työskenteleviä työntekijöitä tekemään yhteistyötä	●	●	
Yrityksen videoportaali yritysvideoiden lataamiseen ja jakamiseen koko yrityksessä	●		
Mukautettu haku ja etsintä kaikissa Office 365 -sovelluksissa Office Graph -toiminnolla	●		
Sovellusten hallinta yritystasolla: ryhmäkäytäntö, telemetria ja aktivointi jaetussa tietokoneessa	●		
Omatoiminen liiketoimintatietojen hallinta tietojen etsimiseen, analysoimiseen ja visualisoimiseen Excelissä	●		

Vaatimustenmukaisuus ja tietosuoja mukaan lukien sähköpostin ja tiedostojen lakisääteinen säilytys, oikeuksienhallinta ja tietojen menetyksen estäminen			
eDiscovery-keskus, työkalut vaatimustenmukaisuuden helpottamiseen			

Asiakkaan ollessa voittoa tavoittelematon organisaatio sille hankitaan Non-profit Agreement -nimikkeellä olevat lisenssit, jotka maksavat puolet normaalihintaisista palvelupaketeista. Non-profit Agreement -sopimus kestää kaksi vuotta, minkä jälkeen se on mahdollista uusia saatavilla olevien sopimusmallien mukaan. Non-profit Agreement -sopimus päättyi asiakkaalla vuonna 2014, jolloin se vaihdettiin Charity licenses -sopimukseksi. Se on voimassa kaksi vuotta.

6 Palvelininfrastruktuurin suunnittelu

Asiakkaan palvelinympäristö suunnitellaan uudelleen käyttäen ADFS-ympäristöä Office 365:n käyttöä varten tarjoten keskitetyn käyttäjä- ja työasemahallinnan. ADFS-ympäristö vaatii toimiakseen Active Directory Domain Controller -palvelimen, Active Directory Federation Service -palvelimen, Active Directory Federation Proxy -palvelimen ja Directory Synchronization tool -työkalun. ADFS-ympäristössä käyttäjät pääsevät kirjautumaan Office 365 -palveluihin samalla käyttäjätunnuksella kuin AD-ympäristöön. SSO taas mahdollistaa kertakirjautumisen, jonka jälkeen todennustiedot lähetetään automaattisesti niitä tarvitseville palveluille [6].

6.1 Active Directory -palvelimen suunnittelu

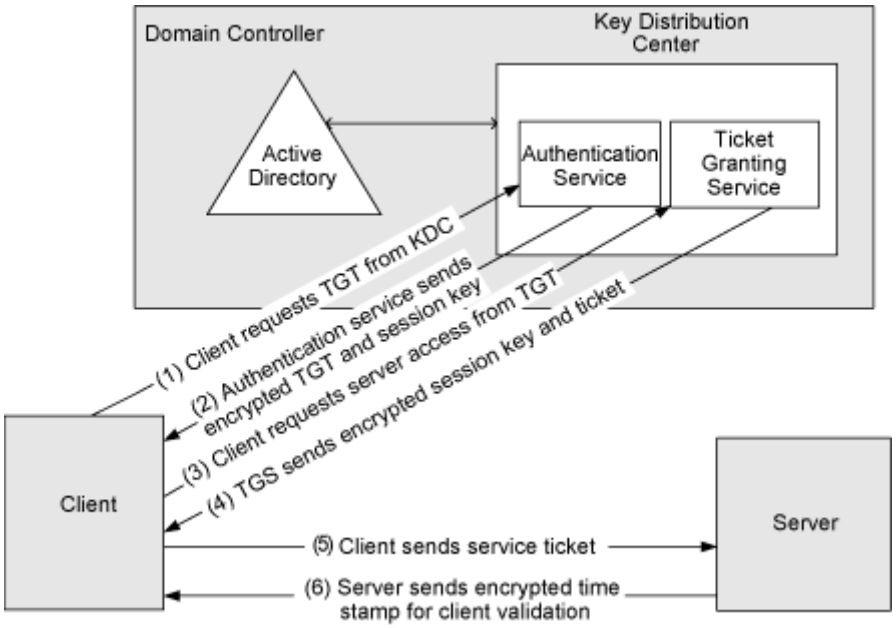
Active Directory -palvelin nimetään AD1-palvelimeksi, jonka rooli on toimia toimialueen pääsääntöisenä ohjauskoneena. Se sisältää toimialueen käyttäjä- ja työasema-objektien tiedot ja käytäntöjen hallinnan. Se toimii myös toimialueen sertifikaattien julkaisu- ja jakelupalvelimena ja ensisijaisena sisäisen verkon nimipalvelimena. AD01-palvelimelle liitetään erillinen kiintolevy tiedostojakoa varten. Active Directory -palvelimelle

asennetaan Windows Server 2012 64bit Datacenter -käyttöjärjestelmä seuraavilla rooleilla, palveluilla ja työkaluilla:

- Active Directory Certificate Services
- Active Directory Domain Services
- DNS Server
- File and Storage Services.

6.2 Active Directory Federation Services 2.0 -palvelun suunnittelu

Active Directory Federation Services 2.0 -palvelu mahdollistaa kertakirjautumisen Office 365 -palveluihin sisä- ja ulkoverkosta AD-käyttäjätunnuksella. ADFS 2.0 tukee useita todennustapoja, mutta yleisin niistä on Kerberos-todennus. Sitä käytettiin myös projektin ADFS 2.0 -palvelussa. Kerberos-protokolla todentaa käyttäjät claims based -tyypppisesti. Kerberos-todennus myöntää autentikaation pyytäjälle tiketin ja mikäli se sisältää oikeat tunnukset, käyttäjä on oikeutettu kirjautumaan palveluun kuvan 3 mukaisesti. [7.]

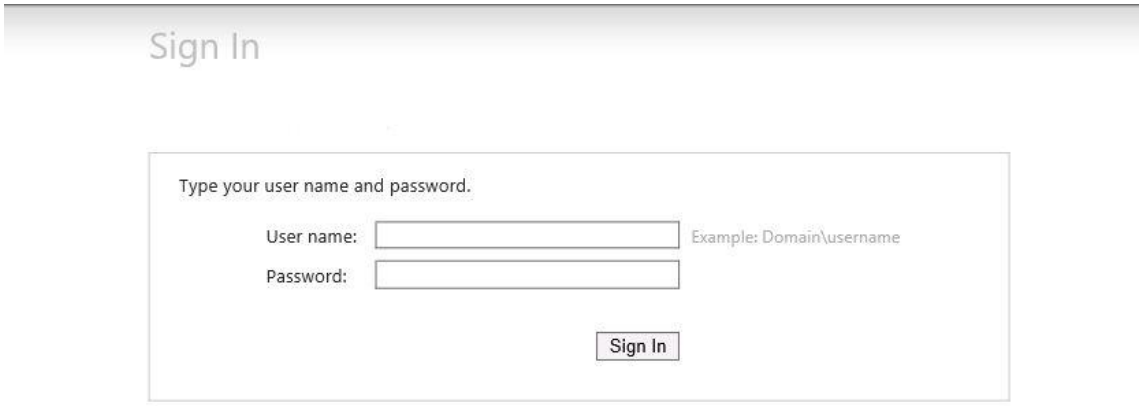


Kuva 3. Kerberos-todennus [7].

ADFS-federointi luo luottamussuhteen Office 365 -palvelun ja Active Directory -palvelimen välille. ADFS-federoinnin avulla Office 365:n käyttäjähallinta tapahtuu Active Directory -palvelun kautta. Directory Synchronization -työkalu ylläpitää käyttäjien synkronoimisen Office 365 -palveluun.

Käyttäjien tunnistus Office 365 palveluun ohjautuu sisäverkossa ollessa ADFS-palvelimelle, joka todentaa käyttäjän Active Directory -palvelusta. Mikäli todennus onnistuu, käyttäjä pääsee kirjautumaan Office 365 -palveluun. Ulkoverkon kautta käyttäjät todentuvat ADFS proxy -palvelimelle, josta todennuspyyntö siirtyy ADFS-palvelimelle ja sieltä edelleen Active Directory -palveluun. Office 365 -palveluun määritetty federoitu toimialue ohjautuu automaattisesti tunnistautumispalvelimelle.

ADFS-palvelimille asennetaan web-palvelinohjelmisto IIS (Internet Information Services) sekä Office 365:en HTTPS (Hypertext Transfer Protocol Secure) -tunnistautumissivua varten SSL (Secure Sockets Layer) -varmenne. Julkiverkosta ADFS Proxy -palvelin vastaa Office 365 -palvelun tunnistautumissivulla HTTPS-pyyntöihin kuvan 4 osoittamalla tavalla.



Kuva 4. Office 365 palveluun kirjautuminen web-palvelimen kautta.

ADFS 2.0 -palvelua varten määritetään kaksi palvelinta. Sisäverkon käyttäjän todentava ADFS 2.0 -palvelin ja ulkoverkon käyttäjien todentava ADFS 2.0 Proxy -palvelimen. ADFS-palvelua varten on mahdollista lisätä redundanssia ja kuormitusta varten ADFS-klusteri, mutta kyseisen asiakkaan tapauksessa päädyttiin olemaan ottamatta tätä käyttöön tarpeettomana. Lisäksi tietoturvan parantamista varten on suositeltavaa asentaa ADFS 2.0 Proxy -palvelin DMZ-alueelle (Demilitarized Zone) eristämällä siten palvelin sisäverkosta.

Directory Synchronization -työkalu on Microsoftin suositusten mukaan asennettava palvelimelle, johon ei ole asennettu toimialueen ohjauspalvelimen roolia. Asiakkaan toiveiden mukaisesti pidettiin palvelinmäärä mahdollisimman vähäisenä, Directory Synchronization -työkalu jouduttiin asentamaan ADFS 2.0 Proxy -palvelimelle. ADFS 2.0 Proxy -palvelimelta on julkiverkkoon HTTPS-portti auki.

Directory Synchronization -työkalun tarkoitus on synkronoida AD-käyttäjät Office 365 -palveluun. Directory Synchronization -työkalulla on mahdollista synkronoida 50 000 AD-objektia, määrittää synkronoinnin aikaväli ja valita synkronoitavat kohteet [8].

Directory Synchronization -työkalu on ladattavissa verkkosoitteesta http://www.microsoft.com/en-us/download/details.aspx?id=22042 ja asennetaan määritetylle palvelimelle.

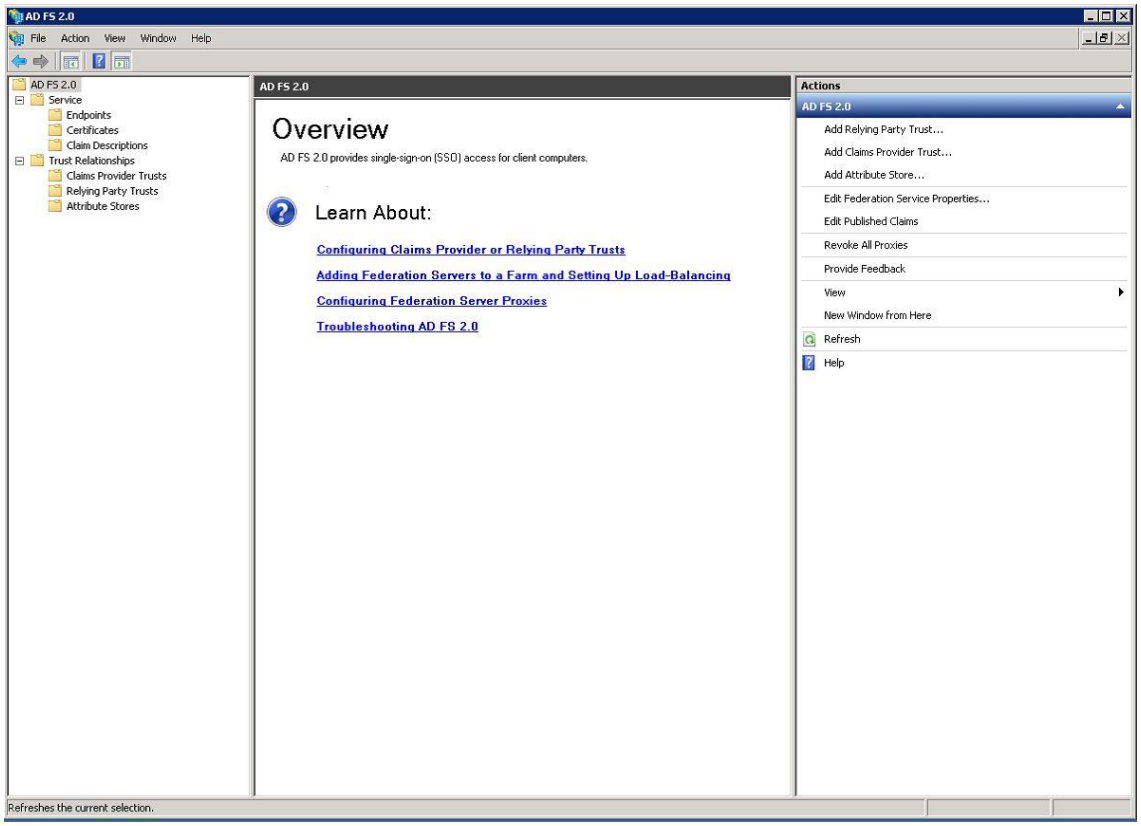
6.2.1 ADFS 2.0 -palvelimen suunnittelu

ADFS 2.0 nimetään ADFS1 -palvelimeksi. Sille asennetaan Windows Server 2008R2 -käyttöjärjestelmä seuraavilla rooleilla, palveluilla ja työkaluilla:

- Active Directory Domain Services
- DNS Server
- File Services
- Print and Document Services
- Web Server (IIS)
- ADFS 2.0
- Microsoft Online Services Sign-In Assistant
- Windows Powershell Microsoft Online Services -moduuli.

ADFS 2.0 -asennuspaketti ladataan erikseen Microsoftin sivuilta ja asennetaan palvelimelle. Kuvassa viisi on esitetty ADFS 2.0 hallintapaneeli.

ADFS1 -palvelin määritetään toimialueen toissijaiseksi ohjauspalvelimeksi ja nimipalvelimeksi. Lisäksi siihen asennetaan tulostuspalvelu.



Kuva 5. ADFS 2.0 -hallintapaneeli.

6.2.2 ADFS 2.0 Proxy-palvelimen suunnittelu

ADFS 2.0 Proxy -palvelin nimetään ADFSPROXY-palvelimeksi. ADFSPROXY-palvelimelle asennetaan Windows Server 2008R2 -käyttöjärjestelmä seuraavilla rooleilla, palveluilla ja työkaluilla:

- Web Server (IIS)
- Directory Synchronization tool
- ADFS 2.0 Proxy
- Microsoft Online Services Sign-In Assistant
- Windows Powershell Microsoft Online Services -moduuli.

6.3 SQL-tietokantapalvelimen suunnittelu

SQL-tietokantapalvelin nimetään SQL1-palvelimeksi. SQL1-palvelimelle asennetaan Windows Server 2012 64-bit Datacenter -käyttöjärjestelmällä seuraavilla rooleilla, palveluilla ja työkaluilla:

- IIS
- NAP
- Remote Desktop Services
- SQL Server 2012 Express.

6.4 Microsoft Direct Access 2012:n suunnittelu

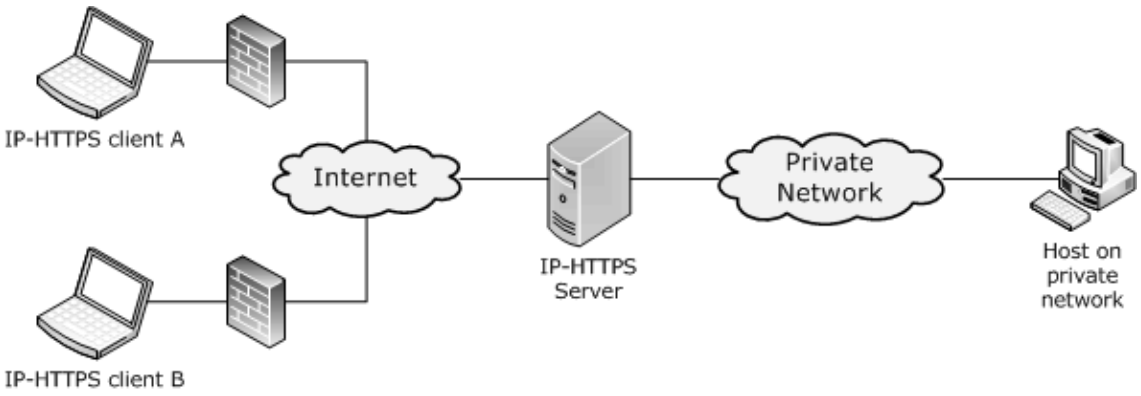
Microsoft Direct Access 2012 -palvelin nimetään DA1-palvelimeksi, jolle asennetaan Windows Server 2012 Datacenter -käyttöjärjestelmä seuraavilla rooleilla, palveluilla ja työkaluilla:

- IIS
- Remote Access.

Direct Access 2012:n asennukseen käytettiin verkossa olevaa asennusohjetta, joka ohjeistaa palvelun asennuksen kohta kohdalta [9]. Direct Access 2012 vaatii työaseman käyttöjärjestelmältä Windows 7 Enterprise ja Ultimate tai Windows 8 Enterprise -version ja palvelimelta Windows Server 2008R2 tai Windows Server 2012 -version.

Direct Access 2012 luo palveluun liitetylle työasemalle työaseman käynnistyksen yhteydessä suojatun verkkoyhteyden julkisesta verkosta yrityksen sisäverkkoon IPv6 (Internet Protocol version 6)-verkon yli. Toimiakseen IPv4 verkossa, Direct Access 2012 -palvelussa käytettiin IP-HTTPS-tunnelointiprotokollaa, joka kapseloi IPv4 (Internet Protocol version 4)-paketin IPv6-paketiksi. Se tukee tämän lisäksi Teredo ja 6to4 tunnelointiprotokollia. Direct Access 2012 -palvelu vaatii toimiakseen IPv6-verkon. Direct Access 2012 -palvelu vaatii toimiakseen palvelinverkolta IPv6-verkon.

IP-HTTPS-tunnelointiprotokolla mahdollistaa symmetrisen linkin käyttäen multicast- ja neighbor discovery -ominaisuuksia. IP-HTTPS perustuu PPP (Point-to-Point) -protokollaan joka käyttää staattista verkon osoitusta OSI (Open Systems Interconnection model)-mallin verkkokerroksen ja siirtokerroksen välissä [10]. Kuvassa 6 on esitetty työasemien yhteys IP-HTTPS-palvelimeen.



Kuva 6. Työasemien yhteys IP-HTTPS-palvelimeen [10].

Työasemien Direct Access -yhteys kytkeytyy pois päältä, kun työasema on yhteydessä yritysverkkoon ja kytkeytyy päälle, kun työasema on yritysverkon ulkopuolella. Direct Access -asiakasohjelma tunnistaa olevansa ulkoverkossa, mikäli se ei saa yhteyttä HTTPS -protokollalla Direct Access 2012 palvelimen ylläpitämään URL:ään, joka on kytketty yrityksen sisäverkkoon [11].

7 Ensimmäisen vaiheen toteutus

Projektin toteutus työstetään projektisuunnitelman mukaisesti. Asiakkaan kanssa sovitaan aikataulut ja ilmoitetaan uusien palveluiden käyttöönottamisesta koituva käyttökatkos. Palvelininfrastruktuurin ja palvelinverkon rakentamisen jälkeen käydään läpi asiakkaan toimipisteissä sijaitsevat työasemat läpi.

7.1 Palvelinverkon määritys

Projektin ensimmäisen vaiheen palvelimet määritetään Comspot Oy:n palvelinkeskuksessa määritettyyn palvelinverkkoon. Palvelinverkkoon lisätään

asiakkaalle dedikoitu VLAN (virtual local area network), johon sisäverkon IP-avaruus määritetään. Julkiverkon IP-avaruus määritetään Comspot Oy:n tarjoamista osoitteista. Palvelinkeskuksen palomuureihin määritetään palvelinympäristön vaatimat palomuuri ja NAT (Network address translation) -säännöt.

7.2 Palvelininfrastruktuurin ja ADFS 2.0 -palvelun asennus

Palvelininfrastruktuuri suunnitellaan toimimaan ADFS 2.0 -ympäristöä varten, johon asennetaan sen vaatimat palvelimet ja niiden palvelut.

7.2.1 AD1-palvelimen asennus

AD1-palvelin asennetaan XenServer-virtualisointialustalle. Palvelimelle määritetään kaksi VCPU (Virtual Central processing unit) -prosessoria, 4096 MB keskusmuistia, 40 GB SAS-kiintolevy, 250 GB SAS-kiintolevy ja virtuaalinen verkkokortti. Käyttöjärjestelmäksi asennettiin Windows Server 2012 Datacenter 40 GB SAS -kiintolevylle ja otettiin suunnitelman mukaiset roolit ja palvelut käyttöön. AD1 -palvelin toimii toimialueen ensisijaisena ohjaus-, DNS (Domain Name System)- ja varmennusten jakelupalvelimena.

AD1-palvelimen toimialueen lisäämisen jälkeen vanhasta palvelimesta käytiin läpi validit käyttäjät ja lisättiin uuteen toimialueeseen. Active Directory Domain Functional Level ja Forest Functional Level asetettiin Windows Server 2008:n R2-tasolle, joka mahdollistaa Windows 2008 R2 -käyttöjärjestelmän käytön toimialueen ohjauspalvelimena [12].

Vanhalla palvelimella oli käytössä verkkojako, johon käyttäjät tallensivat tietojaan. Tiedot siirrettiin AD1 -palvelimeen liitettyyn 250 GB SAS -kiintolevylle, joka toimii käyttäjien tietojen tallennuspaikkana. Asiakkaan toimipisteen hitaan internetyhteyden ja suuren datamäärän vuoksi jouduimme aikataulussa pysyäksemme siirtämään vanhan palvelimen datan ulkoiselle kiintolevylle, josta se siirrettiin palvelinsalissa palvelimelle.

Toimialueen käyttäjien ja -työasemien hallintaa varten OU-rakenne luotiin uudelleen käyttäen mallina asiakkaan organisaation rakennetta. Käyttäjille ja työasemille luotiin

Security Group -ryhmät eri osastojen tai erityisryhmien oikeuksien hallintaa varten. Ryhmäkäytännöt käyttäjille ja työasemille jaettiin Group Policy Managementin kautta.

7.2.2 ADFS1-palvelimen asennus

ADFS1-palvelin asennettiin XenServer-virtualisointialustalle. Palvelimelle määritetään kaksi VCPU -prosessoria, 2048 MB keskusmuistia, 40 GB SAS -kiintolevy ja virtuaalinen verkkokortti. Käyttöjärjestelmäksi asennettiin Windows Server 2008 R2 ja otettiin suunnitelman mukaiset roolit ja palvelut käyttöön. ADFS1-palvelin toimii toimialueen toissijaisena ohjaus- ja DNS-palvelimena sekä ensisijaisena ADFS 2.0 -palvelun palvelimena.

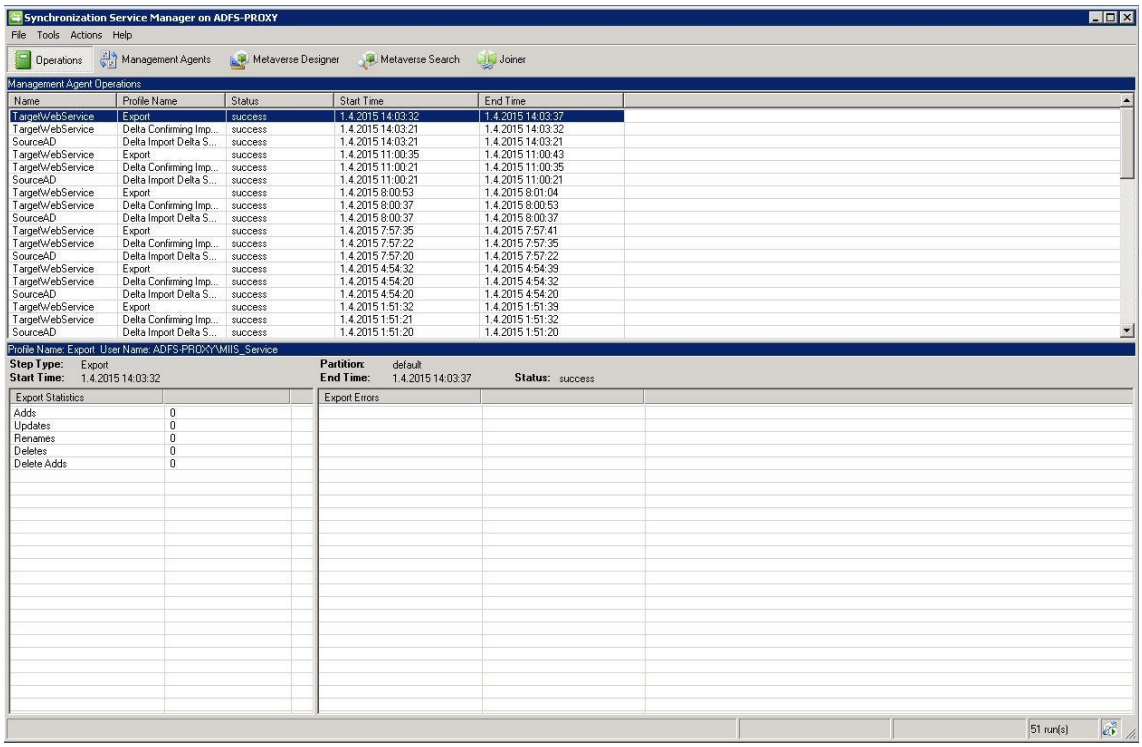
7.2.3 ADFSPROXY-palvelimen asennus

ADFSPROXY- palvelin asennettiin XenServer-virtualisointialustalle. Palvelimelle määritetään kaksi VCPU -prosessoria, 2048 MB keskusmuistia, 40 GB SAS -kiintolevy ja virtuaalinen verkkokortti. Käyttöjärjestelmäksi asennettiin Windows Server 2008 R2 ja otettiin suunnitelman mukaiset roolit ja palvelut käyttöön. ADFSPROXY-palvelin toimii toimialueen ADFS 2.0 Proxy -palvelimena.

Directory Synchronization -työkalun asennusohjelma luo ADFSPROXY-palvelimelle seuraavat ryhmät, joilla hallitaan Directory Synchronization -työkalua:

- MIISAdmins
- FIMSyncBrowse
- FIMSyncJoiners
- FIMSyncOperators
- FIMSyncPasswordSet.

MiisAdmins -ryhmä on työkalun yleinen järjestelmänvalvojan ryhmä, johon järjestelmänvalvojan käyttäjätunnus on liitetty. Kuvassa 7 on esitetty Directory Synchronization -työkalun hallintapaneeli.



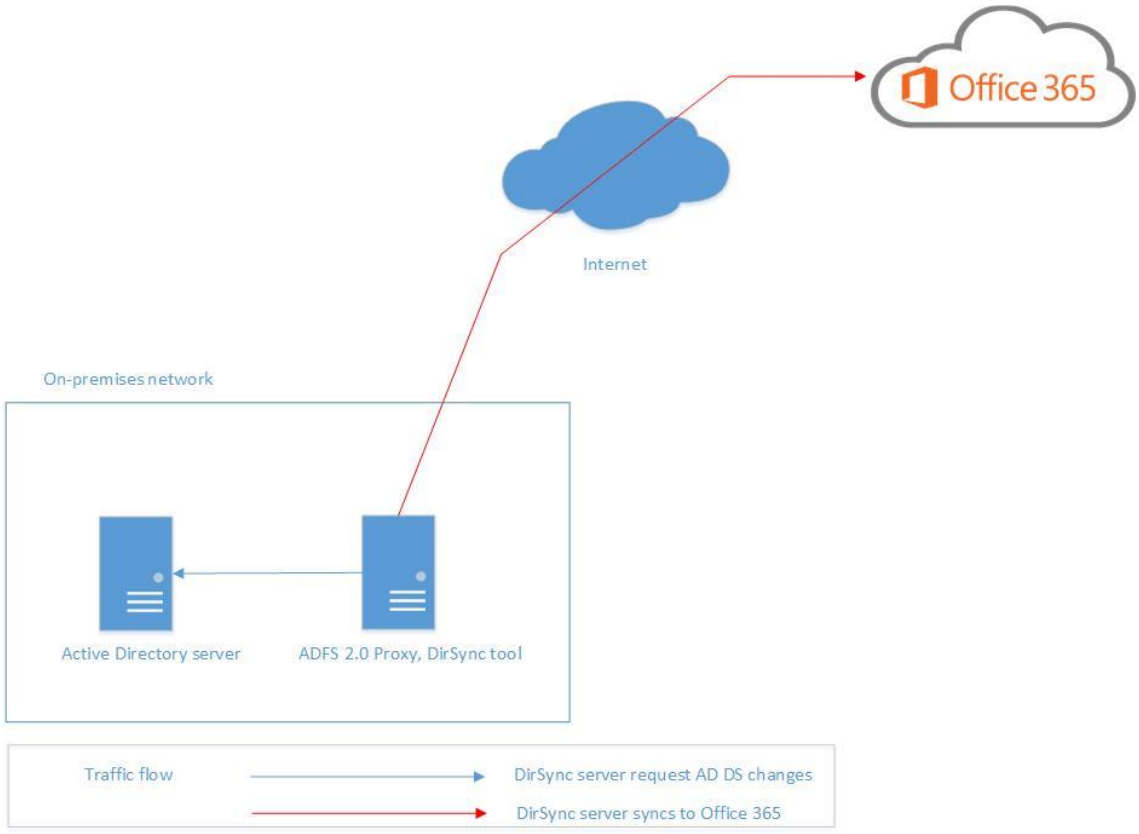
Kuva 7. Directory Synchronization -työkalun hallintapaneeli.

Directory Synchronization -työkalu synkronoi Office 365 -palveluun AD-objektit seuraavien AD-objektien attribuuttien mukaisesti [13, s.167–169]:

- userPrincipalName (UPN)
    - Active Directory -palvelun käyttäjänimen ensisijainen tunnistusnimi, joka koostuu kirjautumistunnuksesta ja toimialueen nimestä [14].
- sAMAccountNAME
    - Active Directory -palvelun käyttäjän kirjautumisnimi, jota käytettiin Windows NT 4.0, Windows 95, Windows 98, and LAN Manager -käyttöjärjestelmissä [15].

- proxyAddresses
    - osoite, jolla Microsoft Exchange Server sähköpostin käyttäjä tunnistetaan ulkopuolisissa sähköpostijärjestelmissä [16].
- givenName
    - AD-käyttäjän etunimi
- sn
    - AD-käyttäjän sukunimi
- mailNickname
    - sähköpostiosoitteen alias
- mail
    - sähköpostin osoite.

Ennen hakemistosynkronoinnin aloittamista AD-objektien attribuutit on varmistettava että kyseiset attribuutit ovat määritetty AD-objekteihin. UPN-attribuutin toimialueen on oltava sama kuin Office 365 -palveluun määritetty toimialue. Mikäli AD1-palvelimen toimialue on eri kuin Office 365 -palveluun määritettävä verkkotunnus, sitä varten on lisättävä Active Directory -palvelimen Active Directory Domains and Trust -hallinta-paneeliin alternative UPN suffix vastaamaan Office 365:n verkkotunnusta [17, s.111–112]. Tämän jälkeen valitaan Directory Synchronization -työkalulla synkronoitavat AD-objektit ja suoritetaan synkronointi. Kuvassa 8 on esitetty työkalulla tehty synkronointi-tapahtuma Active Directory -palvelimesta Office 365 -palveluun.



Kuva 8. Directory Synchronization [18].

7.2.4 ADFS 2.0 -palvelun määrittäminen

ADFS 2.0 ja ADFX 2.0 Proxy -palvelinten asennuksien jälkeen määritetään federointi ja SSO-palvelu päälle käyttämällä Windows Powershell Microsoft Online Services -moduulia ADS 2.0 -palvelimella ja suorittamalla seuraavat komennot [19, s.123–124]:

- ”$cred=Get-Credential” määritetään muuttujalle ”$cred” Office 365 -palvelun järjestelmänvalvojan oikeudet omaavat käyttäjätunnukset.

- ”Connect-MsolService -Credential $cred” yhdistetään Office 365 -palveluun.

- “Set-MsolAdfscontext -Computer <ADFS 2.0 primary server>” määritetään ADFS 2.0 -primääripalvelin käyttäen ADFS 2.0 -palvelimen FQDN (Fully qualified domain name)-nimeä.

- “New-MsolFederatedDomain -DomainName <domain>” määritetään federoitu toimialue Office 365 palveluun. Toimialue on lisättävä julkiseen DNS-palveluun.

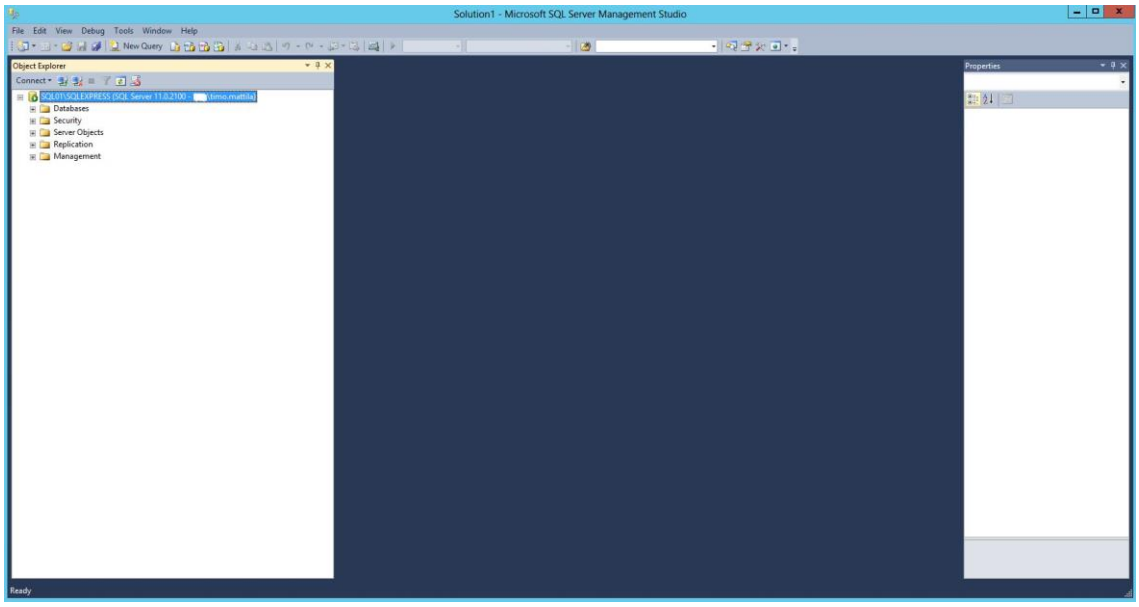
- ”New-MsoldFederatedDomain” määritetään toisen kerran samalla toimialueen nimellä, jolla viimeistellään prosessi.

7.2.5 SQL1-palvelimen asennus

SQL-palvelin asennettiin XenServer-virtualisointialustalle. Palvelimelle määritetään kaksi VCPU -prosessoria, 4096 MB keskusmuistia, 60 GB SAS kiintolevy, 10 GB SAS kiintolevy, 60 GB SAS kiintolevy ja virtuaalinen verkkokortti. Käyttöjärjestelmäksi asennettiin Windows Server 2008 R2 ja otettiin suunnitelman mukaiset roolit ja palvelut käyttöön.

Comspot Oy asensi SQL- palvelimen alustan, tietokannan ajastetun varmuuskopioinnin ja käyttöoikeudet. Tietokannan data tallennetaan 10 GB SAS-kiintolevylle ja tietokannan varmuuskopiointi suoritetaan toiselle 60 GB SAS-kiintolevylle.

SQL-tietokantaa käyttävän sovelluksen asensi sovelluksen kehittäjä. Ohjelmisto jaettiin käyttöön määrittämällä pikakäynnistyskuvake ohjelmaa käyttävien henkilöiden työasemille. Kuvassa 9 on esitetty Microsoft SQL Server Management Console -hallintapaneeli.

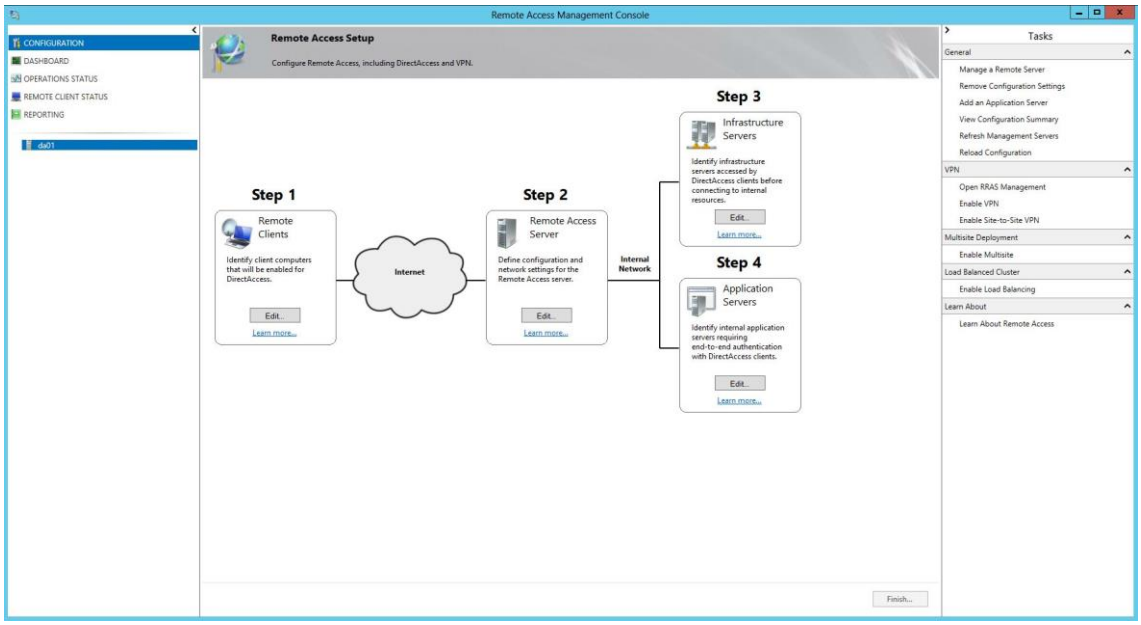


Kuva 9. Microsoft SQL Server Management Console.

7.2.6 DA01-asennus

DA01-palvelin asennettiin XenServer-virtualisointialustalle. Palvelimelle määritetään kaksi VCPU -prosessoria, 1024 MB keskusmuistia, 40 GB SAS-kiintolevy ja virtuaalinen verkkokortti. Käyttöjärjestelmäksi asennettiin Windows Server 2012 Datacenter ja otettiin suunnitelman mukaiset roolit ja palvelut käyttöön.

Direct Access 2012 -palvelun vaatii DA-palvelimen käyttöjärjestelmän palomuurin päälle sekä portin 443 auki verkkoinfrastruktuurin palomuurissa. Direct Access 2012 Wizard luo tarvittavat palomuurisäännöt käyttöjärjestelmän palomuurille sekä luo self-signed -varmenteen IP-HTTPS-protokolla varten. Lisäksi siinä määritetään Direct Accessin verkkotopologia, käyttäjäryhmä Direct Access -asetusten asentamiselle, toimivuus Windows 7 -käyttöjärjestelmässä ja NLS (Network Location Server). Kuvassa 10 on esitetty Direct Access 2012 -palvelun Remote Access Management Console -hallintapaneeli.



Kuva 10. Remote Access Management Console.

Työasemien tunnistamista varten Direct Access 2012 -palveluun luodaan työasema ja palvelinvarmenteet Active Directoryn Certification Authority -hallintapaneelista. Työasemavarmenteen automaattinen asennus määritetään päälle toimialueen työasemille oletus-GPO:n (Group Policy Object) kautta.

Direct Access 2012 -asennuksessa on tarkasti seurattava ohjeita ja testaa se testi-ympäristössä. Väärin asennettuna se rikkoo työasemien toimialueen yhteyden, jolloin työasemat pitää korjata manuaalisesti yksi kerrallaan.

7.3 Office 365:n käyttöönotto

Office 365:n tilaus luotiin asiakkaalle tekemällä kokeiluversio Office 365:n tilauksesta, jossa palveluun luodaan järjestelmänvalvojan käyttäjätunnus ja verkkotunnus esimerkkimuodon mukaisesti käyttäjänimi@toimialue.onmicrosoft.com.

Tämän jälkeen lisätään varsinainen toimialue, jonka omistajuus varmistetaan julkisen DNS (Domain Name System)-palvelun kautta. Sähköpostimigraation jälkeen palveluun lisätään sähköposti-ohjauksen tietueet ja Lync-ohjelman tietueet [20]. Kuvassa 11 on esitetty Office 365 palvelun lisättävät DNS-tietueet.

Exchange Online

TYPE	PRIORITY	HOST NAME	POINTS TO ADDRESS	TTL
MX	0	@	comspot-fi.mail.protection.outlook.com	1 Hour
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour

TYPE	TXT NAME	TXT VALUE	TTL
TXT	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour

Microsoft Lync

TYPE	SERVICE	PROTOCOL	PORT	WEIGHT	PRIORITY	TTL	NAME	TARGET
SRV	_sip	_tls	443	1	100	1 Hour	@	sipdir.online.lync.com
SRV	_sipfederationtls	_tcp	5061	1	100	1 Hour	@	sipfed.online.lync.com

TYPE	HOST NAME	POINTS TO ADDRESS	TTL
CNAME	sip	sipdir.online.lync.com	1 Hour
CNAME	lyncdiscover	webdir.online.lync.com	1 Hour

Additional Office 365 records

TYPE	HOST NAME	POINTS TO ADDRESS	TTL
CNAME	msoid	clientconfig.microsoftonline-p.net	1 Hour

Kuva 11. Office 365 -palvelun lisättävät DNS-tietueet.

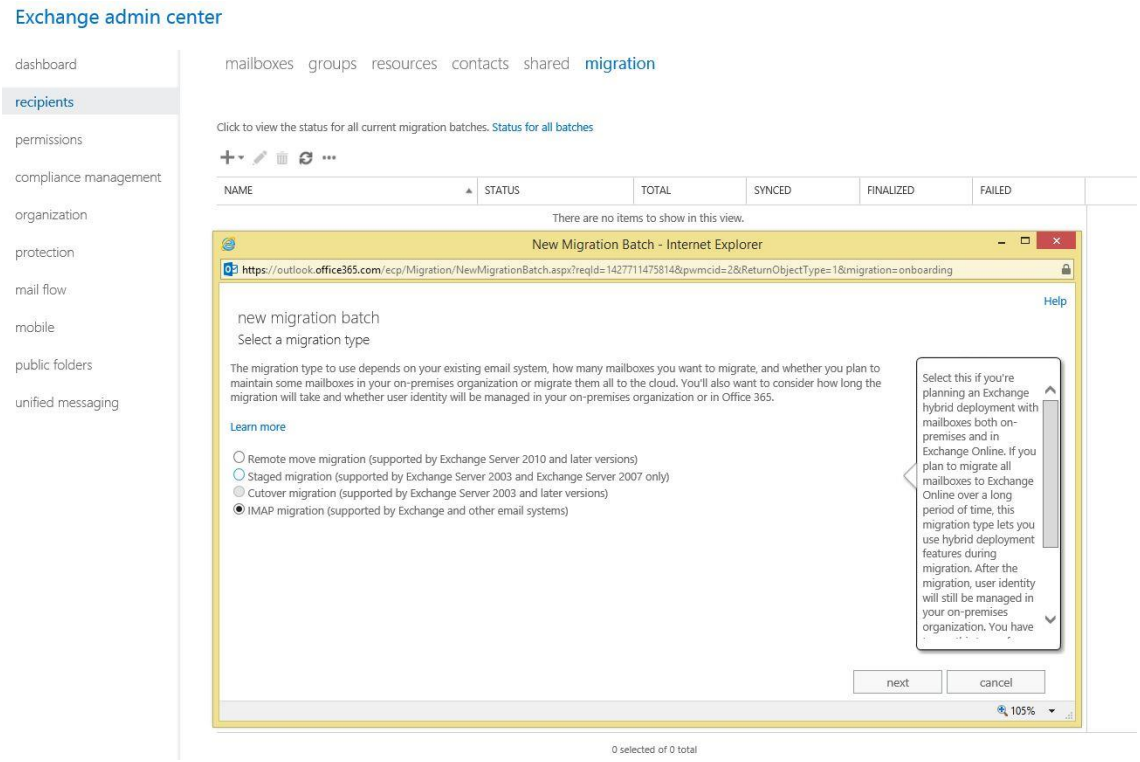
Office 365:n sähköpostimigraatio

Sähköpostimigraatio suoritetaan Office 365 -palvelun tarjoamalla migraatiotyökalulla. Migraatiotyökalulla on mahdollista tehdä migraatioita Exchange- ja IMAP-protokollaa tukevista sähköpostijärjestelmistä. Sähköpostimigraatioita varten kartoitetaan siirrettävät sähköpostitilit ja niiden koko. Lisäksi arvioidaan käytössä olevan verkkoyhteyden mukaan siirtoon kuluva aika.

Sähköpostimigraatioon käytettiin Office 365 -sähköpostimigraatiotyökalun IMAP (Internet Message Access Protocol) -tyyppistä migraatiota. Se siirtää käyttäjän sähköpostit Office 365 -sähköpostitilille. Käyttäjät synkronoidaan Active Directory -ympäristöstä Office 365 -palveluun Directory Synchronization -työkalulla ja niille määritetään palvelupaketit. Siirrettävistä käyttäjistä luodaan CSV (Comma-separated values) -tyyppinen tiedosto, jota käytetään sähköpostimigraatiotyökalussa tunnistamaan siirrettävät sähköpostitilit. CSV-tyyppinen tiedosto on taulukkorakenteinen tekstitiedosto,

jonka rivien arvot ovat eroteltu toisistaan erotinmerkillä, yleensä pilkulla [21]. CSV -tiedoston lisäämisen jälkeen käynnistetään sähköpostimigraatio.

Migraation jälkeen Office 365 -palvelun sähköpostiohjauksen tietueet lisätään DNS-palveluun. Sähköpostimigraatio suoritettiin projektin loppuvaiheessa palvelinympäristön rakentamisen jälkeen. IMAP (Internet Message Access Protocol) -tyyppistä sähköposti-migraatiota käytettiin myös projektin toisen vaiheen sähköpostimigraatiossa. Kuvassa 12 on esitetty Office 365 -sähköpostimigraatiotyökalu.



Kuva 12. Office 365 -sähköpostimigraatiotyökalu.

7.4 VPN-tunnelointi

Asiakkaan päätoimiset toimipisteet on liitetty asiakkaan käytössä olevaan MPLS-verkkoon. Projektin ensimmäisessä vaiheessa asiakkaan toimipisteisiin asennettiin Ciscon verkkolaitteilla Site-to-site VPN-yhteys Comspot Oy:n palvelinsalin ja asiakkaan toimipisteiden väliin. Site-to-site VPN-yhteys muodostaa suojatun verkkoyhteyden

tunnelointiprotokollalla kahden eri verkkolaitteen välille esimerkiksi suojaamattoman Internet-yhteyden yli [22].

Asiakkaan ensimmäisen työvaiheen palvelinten verkkoinfrastruktuuri luotiin Comspot Oy:n palvelinsaliin ja määritettiin niille tarvittavat palomuurisäännöt. Asiakkaan toisen toimialueen verkkoliikenne toimii MPLS-verkon kautta. Asiakkaan työasemille asennettiin VPN-asiakasohjelma, toimimaan varayhteytenä, mikäli Direct Access 2012 -yhteys lakkaa toimimasta.

7.5 Windows 7 Enterprisen käyttöönotto työasemissa

Asiakkaan ensimmäisen alaorganisaation työympäristössä oli käytössä 68 työasemaa kahdessa eri työpisteessä, sekä etäkäyttäjien työasemat. Kaikkiin oli asennettu sekalaisesti 32- ja 64-bittisiä Windows XP-, Windows Vista-, Windows 7 Professional -käyttöjärjestelmiä. Työasemat koostuivat kannettavista ja pöytämallisista koneista. Ongelmia käyttöjärjestelmien asennuksissa aiheutti asiakkaan hidas Internet-yhteys sekä erimerkkiset ja -malliset työasemat, joihin täytyi erikseen asentaa laitteiston ajureita. Dokumentaatiota asiakkaan käytössä olevista työasemista ei ollut olemassa.

Työasemien päivitys Windows 7 -käyttöjärjestelmäksi ja liittäminen uuteen toimialueeseen sekä vanhan palvelimen tietojen siirto uudelle palvelimelle ajoitettiin viikonlopuksi, jotta tietojärjestelmien päivityksen aiheuttama katkos ei haittaisi asiakkaan liiketoimintaa.

Windows Intune -palvelusta saatavasta Windows 7 Enterprisen levykuvasta luotiin kustomoitu levykuva, joka sisälsi asiakkaan tarpeita vastaavat toimisto-ohjelmistot, päivitykset sekä muut apuohjelmat. Levykuvan luomiseen käytettiin Windows AIK -työkalua, joka on ladattavissa Microsoftin sivuilta osoitteesta http://www.microsoft.com/en-us/download/details.aspx?id=5753.

Projektissa asennettiin työasemille Windows Intune -asiakasohjelmisto työasemien käyttöjärjestelmien asennuksien yhteydessä. Windows Intunesta määritettiin työasemien Windows Update -käytännöt.

Työasemien profiilien tiedostojen siirrossa käytettiin Windows Easy Transfer -työkalua, joka yksinkertaistaa siirrettävien tietojen prosessia. Uudelleen asennetut työasemat liitettiin uuteen toimialueeseen. Kuvassa 13 on esitetty Windows Easy Transfer -työkalu.

Kuva 13. Windows Easy Transfer -työkalu.

8 Projektin toinen vaihe

Projektin toisessa vaiheessa yhdistettiin asiakkaan toinen tietojärjestelmä projektin ensimmäisessä vaiheessa rakennettuun tietojärjestelmään. Projektin toinen vaihde suoritettiin noin vuoden kuluttua ensimmäisen vaiheen jälkeen. Asiakkaan sähköposti-palvelut Nebula Oy:stä siirrettiin Office 365 -palveluun. Lisäksi Telecitygroup Oy:n palvelinsalista vuokratut palvelimet siirrettiin Comspot Oy:n palvelinsaliin. Tietojärjestelmien yhdistäminen selkeyttää ja tehostaa tietojärjestelmän hallinnointia ja tuo taloudellisia hyötyjä. Projektin toisen vaiheen työasemille ei otettu Windows Intunea käyttöön eikä työasemia siirretty asiakkaan toiveesta Direct Access 2012 -palveluun.

Työasemissa oli F-secure -tietoturvaohjelmisto, ja käyttöjärjestelmät oli asennettu Microsoft Volume Licensing Service Centerin kautta hankituilla lisensseillä.

8.1 Projektin työvaiheet

Projektin toisessa vaiheessa siirrettiin työasemien tiedot samaan tapaan kuin projektin ensimmäisessä vaiheessa ja työasemat liitettiin uuteen toimialueeseen. Osa palvelimista siirrettiin Telecitygroupilta saaduilta virtuaalipalvelinten levykuvilla. Projektin toisen vaiheen työvaiheet on esitetty taulukossa 3.

Taulukko 3. Projektin toisen vaiheen työvaiheet.

Task Name	WBS	Predecessors
Palvelinverkon ja palveluiden yhdistäminen	**0**	
Valmistavat toimenpiteet	**1**	
Siirtoajankohdan kartoittaminen	1.1	
Palvelukatkoksesta tiedottaminen	1.2	
Toimipisteiden työasemien kartoitus	1.3	
Työasemasiirron työjärjestyksen teko	1.4	
Palveluiden siirto	**2**	**1**
MS SQL-tietokannan siirto	**2.1**	
Stanley Security -tietokannan varmuuskopiointi ja siirto	2.1.1	
Stanley Security -ohjelmiston siirto	**2.2**	
Toiminnallisuuden testaaminen	2.2.1	
Abloy-ohjelmiston siirto	**2.3**	
Toiminnallisuuden testaaminen	2.3.1	
Schneider -ohjelmiston siirto	**2.4**	
Toiminnallisuuden testaaminen	2.4.1	
IP-avaruuden uudelleen ohjaus	**2.5**	
Toiminnallisuuden testaaminen	2.5.1	
MPLS-reitityksen ohjaaminen	**2.6**	
Toiminnallisuuden testaaminen	2.6.1	
Palvelinjärjestelmien siirron jälkeiset toimet	**3**	**2**
Office 365 -sähköpostimigraatio	3.1	
Työasemien siirtäminen toimialueeseen	3.2	
Dokumentointi	3.3	

8.2 Projektin toisen vaiheen toteutus

Projektin toinen vaihe sisältää käytössä olevien TelecityGroup Oy:ltä vuokrattujen palvelinten, tietojen ja palveluiden siirron Comspot Oy:n palvelinsaliin sekä toisen alaorganisaation työasemien liittämisen projektin ensimmäisessä vaiheessa rakennettuun toimialueeseen. Asiakkaan toimitiloissa olevien pääsynhallintalaitteisiin asennettua IP-osoitetta ei voitu muuttaa, minkä takia jouduttiin säilyttämään asiakkaan

käytössä oleva IP-avaruus. Käytössä olevan IP-avaruuden laajuuden vuoksi Comspot Oy:n palvelinsaliin asennettiin käyttöön verkkolaite, joka mahdollistaa käytössä olevan MPLS-verkon liittämisen Comspot Oy:n palvelinsaliin, jolloin osa asiakkaan toimitiloihin asennetuista Site-to-site VPN-verkkolaitteista voitiin purkaa. Näin asiakkaan verkkoliikenne ohjautuu täysin käytössä olevan MPLS-verkon kautta.

Stanley Security -ohjelmiston siirto

Asiakkaan käyttämä Stanley Security -turvallisuusvalvontajärjestelmän Microsoft SQL-tietokanta siirrettiin asiakkaan ensimmäisessä vaiheessa asennettuun SQL-palvelimelle, joka käyttää Microsoft SQL Server 2012 Express -tietokantaa. Tietokantaan luotiin tarvittavat käyttäjäoikeudet ja poistettiin tarpeettomat. Ohjelmisto asennettiin SQL-palvelimelle ja yhdistettiin varmuuskopiosta palautettuun tietokantaan. Ohjelmistoa käytetään työasemilta Remote Desktop Services -palvelun kautta. Ohjelmisto testattiin ja todettiin toimivaksi.

Abloy ja Schneider -ohjelmistojen siirto

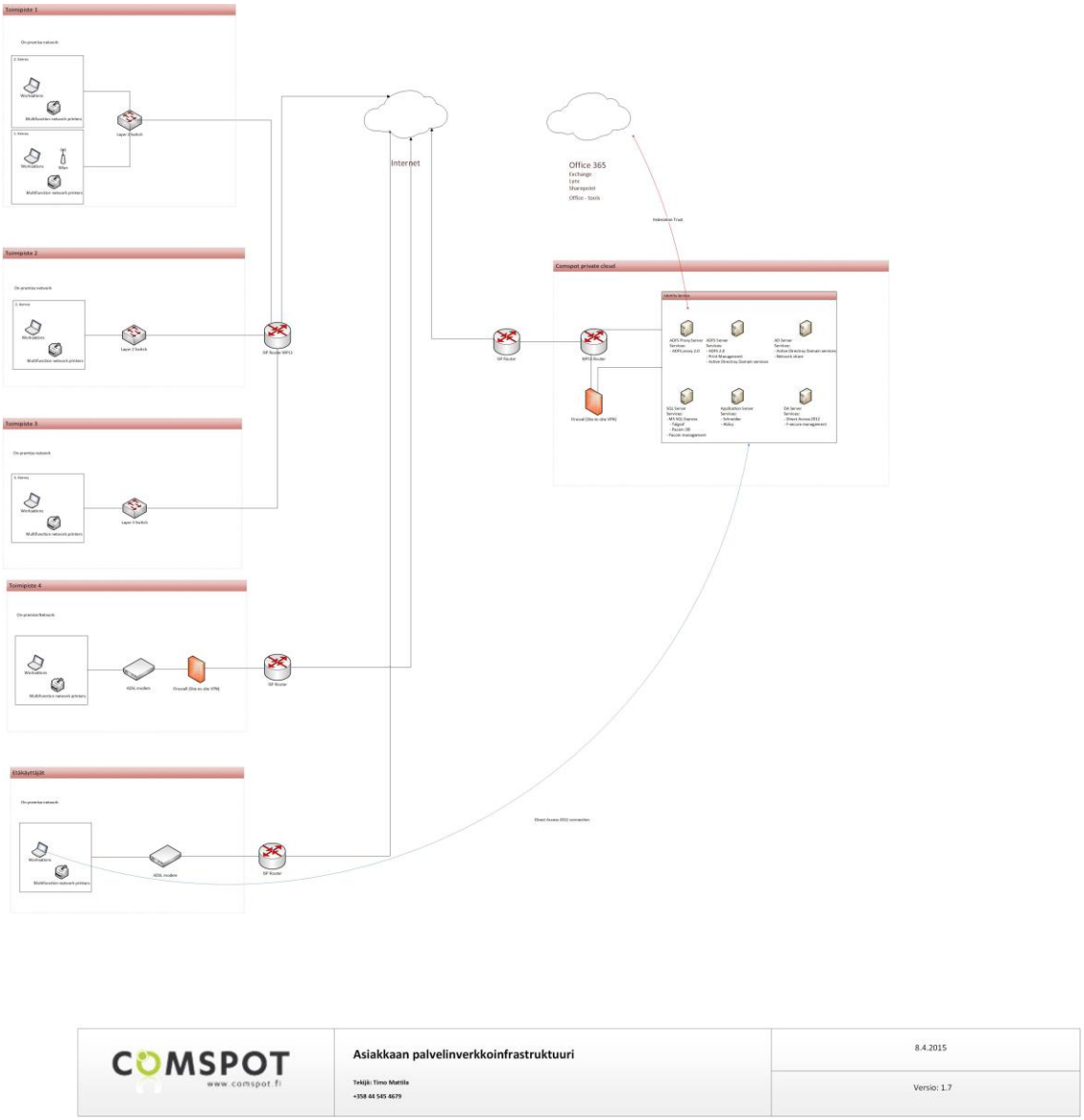
Abloy ja Schneider -ohjelmistoja varten asennettu virtuaalipalvelin asennettiin Telecity-groupilta saadusta levykuvasta Comspot Oy:n palvelinsalin XenServer-virtuaalialustalle. Palvelin poistettiin vanhasta toimialueesta ja siirrettiin uuteen. Ohjelmistot testattiin ja todettiin toimiviksi.

Palvelimelle määritetään kaksi VCPU -prosessoria, 2048 MB keskusmuistia, 50 GB SAS-kiintolevy ja virtuaalinen verkkokortti.

IP-avaruuden uudelleenohjaus ja MPLS-verkon reititys

Telecitygroup Oy toimii asiakkaan palvelinverkon palveluntarjoajana. Suurimpaan osaan asiakkaan toimipisteisiin on asennettu MPLS-kytkimet toisen aliorganisaation eriytettyä tietojärjestelmää varten. Ensimmäisessä vaiheessa rakennettu palvelinverkko ohjataan MPLS-verkkoon ja yhdistetään tietoliikenne. MPLS-verkon palveluntarjoajalle ilmoitetaan tarvittavat IP-avaruuksien lisäykset ja palomuurien porttiavaukset. Comspot Oy:n asentamat Site-to-site-yhteydellä toimivat palomuurit puretaan asiakkaan

toimipisteistä, jotka ovat kytketty MPLS-verkkoon. Kuvassa 14 on esitetty asiakkaalle rakennettu palvelinverkkoinfrastruktuuri.



Kuva 14. Asiakkaan palvelinverkkoinfrastruktuuri.

Projektin toisen vaiheen Office 365 -sähköpostimigraatio

Sähköpostin siirto Office 365 -palveluun suoritettiin samaan tapaan kuin projektin ensimmäisen vaiheen sähköpostimigraatio käyttäen Office 365 -migraatiotyökalua samalla IMAP-tyyppisellä migraatiolla. Ennen sähköpostimigraatioita, toisen

alaorganisaation käyttäjät lisättiin ensimmäisessä vaiheessa rakennettuun AD-ympäristöön, suoritettiin hakemistosynkronointi ja määritettiin Office 365 -palvelupaketit.

Työasemien siirtäminen toimialueeseen

Työasemien siirtämisessä projektin ensimmäisessä vaiheessa luotuun AD-ympäristöön suoritettiin samaan tapaan kuin ensimmäisen alaorganisaation kohdalla. Työasemien tiedot siirrettiin uudelle AD-käyttäjälle Microsoft Easy Transfer -työkalulla, AD-ympäristöön määritettiin GPO-säännöillä tarvittavat verkkojaot ja käyttöoikeudet. Työasemia siirrettiin uuteen toimialueeseen noin 40.

9 Yhteenveto

Insinöörityö oli minulle ensimmäinen suuritöinen asiakasprojekti, johon minut nimettiin projektipäälliköksi. Työni oli alkanut yrityksessä noin puoli vuotta ennen projektin alkua. Työstämistapa oli kehitettävä mahdollisimman selkeäksi ja toimivaksi. Valmista mallia toimitettavalle projektityölle ei ollut saatavilla. Suurimmat haasteet projektissa olivat toimitettavan kokonaisuuden opiskelu ja suunnittelu, sillä yritykselle ei ollut ehtinyt karttua kokemusta vastaavasta hankkeesta.

Projekti onnistui hyvin. Projektin tavoitteena oli uudistaa asiakkaan palvelininfrastruktuuri ja poistaa eriytetyn tietojärjestelmän päällekkäin tarjoamat palvelut, helpottaa asiakkaan palvelininfrastruktuurin hallintaa, lisätä tietoturvaa ja pienentää maksuja. Projektille asetetut tavoitteet saavutettiin. Projektissa pysyttiin annetussa aikataulussa ja asiakas oli tyytyväinen. Projektin päätteeksi asiakkaalle toimitettiin dokumentaation uudesta tietojärjestelmästä ja sen laitteista. Asiakas koki dokumentaation erittäin tärkeänä, sillä aikaisemmasta tietojärjestelmästä sitä ei ollut tehty.

Kireä aikataulu oli haasteellinen eikä asiakkaan hidasta Internet-yhteyttä osattu ottaa tarpeeksi huomioon. Haasteista huolimatta projekti tarjosi paljon käytännön ja teorian koulutusta seuraaviin vastaavanlaisiin projekteihin.

Lähteet

1 Comspot Oy ratkaisut. Verkkodokumentti. Saatavissa: <http://comspot.fi/ratkaisut>. Luettu 13.4.2015.

2 Tutustu Office 365 -palveluun. Verkkodokumentti. Saatavissa: <https://products.office.com/fi-fi/business/explore-office-365-for-business>. Luettu 15.4.2015.

3 Tutustu Windows Intune -palveluun. Verkkodokumentti Saatavissa: <http://www.microsoft.com/fi-fi/windows/windowsintune/faq/faqs/so-what-exactly-is-windows-intune.aspx>. Luettu 15.4.2015.

4 Microsoft Office 365 Deployment Guide for Enterprises. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/hh852466.aspx>. Luettu 1.11.2012.

5 Microsoft Office 365 palvelupaketit. Verkkodokumentti. Saatavissa: <https://products.office.com/fi-fi/business/compare-office-365-for-business-plans>. Luettu 5.4.2015.

6 Office 365 SingleSign-On with AD FS 2.0 whitepaper. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/windowsserver/dd448613.aspx>. Luettu 9.4.2015.

7 Kerberos Explained. Verkkodokumentti. Saatavissa: <https://msdn.microsoft.com/en-us/library/bb742516.aspx>. Luettu 6.4.2015.

8 Deploy Azure Active Directory Sync tool with Office 365. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/dn509521.aspx>. Luettu 13.4.2015.

9 ’Real World’ Direct Access installation using Windows Server 2012. Verkkodokumentti. Saatavissa: <http://blogs.msdn.com/b/canberrapfe/archive/2012/07/12/simple-direct-access-setup-with-windows-server-2012-rp.aspx>. Luettu 8.4.2015.

10 MS-IPHHTPS: IP over HTTPS (IP-HTTPS) Tunneling protocol. Verkkodokumentti. Saatavissa: <https://msdn.microsoft.com/en-us/library/dd358571.aspx>. Luettu 8.12.2015.

11 DirectAccess Client Determines that it is on the Internet when on the intranet. [Verkkodokumentti]. Saatavissa: <https://technet.microsoft.com/en-us/library/ee844105(v=ws.10).aspx>. Luettu 8.4.2015.

12 Understanding Active Directory Domain Services (AD DS) Function Levels. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx>. Luettu 10.4.2015.

13 Microsoft Office 365 Deployment Guide for Enterprises: Appendix F Directory Object Preparation. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/hh852466.aspx>. Luettu 1.11.2012.

14 Add User Principal Names Suffixes. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/cc772007.aspx>. Luettu 12.4.2015.

15 SAM-Account-Name attribute. Verkkodokumentti. Saatavissa: <https://msdn.microsoft.com/en-us/library/ms679635(v=vs.85).aspx>. Luettu 12.4.2015.

16 Proxy-Addresses attribute. Verkkodokumentti. Saatavissa: <https://msdn.microsoft.com/en-us/library/ms679424(v=vs.85).aspx>. Luettu 14.4.2015.

17 Microsoft Office 365 Deployment Guide for Enterprises: Add Alternative UPN Suffix to Active Directory. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/hh852466.aspx>. Luettu 1.11.2012.

18 Deploy Office 365 Directory Syncronization (DirSync) in Microsoft Azure. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/dn635310.aspx>. Luettu 15.4.2015.

19 Microsoft Office 365 Deployment Guide: Enable Single Sign-On. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/hh852466.aspx>. Luettu 1.11.2012.

20 Microsoft Office 365 Deployment Guide for Enterprises: Adding a Domain to Office 365. Verkkodokumentti. Saatavissa: <https://technet.microsoft.com/en-us/library/hh852466.aspx>. Luettu 1.11.2012.

21 Y. Shafranovich. 2005. RFC 4180: Common format and MIME Type for Comma-Separated Values (CSV) Files. Verkkodokumentti. Saatavissa: <https://tools.ietf.org/html/rfc4180#section-1>. Luettu 21.4.2015.

22 Managing Site-to-Site VPNs: The Basics. Verkkodokumentti. Saatavissa: <http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/vpchap.pdf>. Luettu 21.4.2015.